

System and Method for Selectively Confirming Digital Certificates in a Virtual Private Network

ABSTRACT

A system and method for providing multiple virtual private networks (VPNs) from a computer system. Configuration information is maintained for connections, or tunnels, established between a local computer system and a number of remote computer systems. The configuration information includes information about the endpoints, or local-remote computer pairs, policies used to determine preferred access methods for connecting a given pair of computers, pre-shared keys, and digital certificates for providing keys to encrypt and decipher data. A local-remote pair is selected from an endpoints table. A policy corresponding to the selected local-remote pair is selected determining the access method(s) to be attempted in securely connecting the two computer systems. If an access method uses a digital certificate, the corresponding information is retrieved from a digital certificate table. The decision whether to check the digital certification has been revoked is stored in the endpoints table.